

AMENDMENT TO THE CLAIMS

1 1. (Currently Amended) A method of evaluating fraud risk of an electronic commerce
2 transaction, the method comprising the computer-implemented steps of:
3 ~~an apparatus~~ receiving transaction data that defines the electronic commerce transaction;
4 ~~the apparatus~~ determining a first fraud risk score value associated with the electronic
5 commerce transaction based on applying a plurality of tests to the transaction data,
6 wherein each of the plurality of tests determines whether the transaction data
7 appears to represent a genuine transaction based on specified criteria;
8 ~~the apparatus~~ determining a second fraud risk score value associated with the electronic
9 commerce transaction based on a comparison of the transaction data to historical
10 transaction data;
11 ~~the apparatus~~ combining the first fraud risk score value and the second fraud risk score
12 value using a statistical model to result in creating a model score value;
13 ~~the apparatus~~ blending the model score value with one or more merchant-specific
14 threshold values to result in creating and storing a final fraud risk score value for
15 the electronic commerce transaction.

1 2. (Currently Amended) A method as recited in Claim 1, wherein receiving transaction data
2 comprises the steps of ~~the apparatus~~ receiving transaction data that defines the electronic
3 commerce transaction for a particular Internet identity, and wherein determining a second
4 fraud risk score value comprises the steps of ~~the apparatus~~ determining a second fraud
5 risk score value associated with the electronic commerce transaction based on a
6 comparison of the transaction data to historical transaction data for other electronic
7 commerce transactions pertaining to the same Internet identity.

1 3. (Previously Presented) A method as recited in Claim 2, wherein the particular Internet
2 identity comprises a first hash value of an email address of a prospective purchaser
3 carried in combination with a second hash value of a card bank identification number of
4 the prospective purchaser.

1 4. (Previously Presented) A method as recited in Claim 2, wherein the particular Internet
2 identity comprises a first hash value of an email address of a prospective purchaser
3 carried in combination with a second hash value of a card bank identification number of
4 the prospective purchaser and with a third hash value based on a shipping address of the
5 prospective purchaser.

1 5. (Previously Presented) A method as recited in Claim 2, wherein the particular
2 Internet identity comprises a first hash value of an prospective purchaser's host IP
3 address, in combination with a second hash value of an email address of a prospective
4 purchaser carried, in combination with a third hash value of a card bank identification
5 number of the prospective purchaser and a fourth hash value based on a shipping address
6 of the prospective purchaser.

7 6. (Previously Presented) A method as recited in Claim 2, wherein the particular Internet
8 identity comprises a first hash value of a prospective purchaser's hardware device ID
9 value, in combination with a second hash value of either the email address or user ID of
10 the prospective purchaser, in combination with a third hash value of a card bank
11 identification number of the prospective purchaser and with a fourth hash value based on
12 a shipping address of the prospective purchaser.

1 7. (Currently Amended) A method as recited in Claim 1, wherein the step of determining
2 the second fraud risk score value comprises the steps of:
3 the apparatus-retrieving one or more records of historic transaction data pertaining to past
4 transactions associated with the transaction data;

5 when one of the records of historic transaction data is found to contain a fraud list tag,
6 discontinuing further retrieval of such records;
7 ~~the apparatus~~ determining the second fraud risk score value associated with the electronic
8 commerce transaction based on only the retrieved records of historical transaction
9 data in comparison to the transaction data.

1 8. (Currently Amended) A method as recited in Claim 1, wherein the step of determining
2 the second fraud risk score value comprises the steps of:
3 ~~the apparatus~~ retrieving one or more records of historic transaction data pertaining to past
4 electronic commerce transactions associated with the transaction data;
5 when a specified amount of the records of historic transaction data is retrieved and further
6 records of historic transaction data remain to be retrieved, discontinuing further
7 retrieval of such records;
8 ~~the apparatus~~ determining the second fraud risk score value associated with the electronic
9 commerce transaction based on only the retrieved records of historical transaction
10 data in comparison to the transaction data.

1 9. (Currently Amended) The method as recited in Claim 1, wherein the step of blending the
2 model score value comprises the steps of ~~the apparatus~~ blending the model score value
3 with one or more merchant-specific threshold values to result in creating and storing a
4 final fraud risk score value for the electronic commerce transaction and one or more
5 return code values that signal specified risk issues that have been detected with respect to
6 the transaction.

1 10. (Currently Amended) The method as recited in Claim 1, wherein determining the first
2 fraud risk score value comprises the steps of ~~the apparatus~~ determining a first fraud risk
3 score value associated with the electronic commerce transaction based on applying a
4 plurality of tests to the transaction data, wherein one of the plurality of tests determines
5 whether an Internet identity in the transaction data is found in a list of parties to known
6 past fraudulent transactions.

1 11. (Currently Amended) The method as recited in Claim 1, wherein determining the first
2 fraud risk score value comprises the steps of ~~the apparatus~~-determining a first fraud risk
3 score value associated with the electronic commerce transaction based on applying a
4 plurality of tests to the transaction data, wherein one of the plurality of tests determines
5 whether an Internet identity in the transaction data is found in a list of trusted parties.

1 12. (Currently Amended) A method as recited in Claim 1, wherein determining the first
2 fraud risk score value comprises the steps of ~~the apparatus~~-determining a first fraud risk
3 score value associated with the electronic commerce transaction based on applying a
4 plurality of tests to the transaction data, wherein one of the plurality of tests comprises the
5 steps of:
6 ~~the apparatus~~-receiving the text value;
7 for each bi-gram in the text value, ~~the apparatus~~-retrieving from a table of bi-gram
8 probability values a probability value that represents a probability that the bi-gram
9 is found in a genuine text value;
10 ~~the apparatus~~-generating a penalty value when the retrieved probability values indicate
11 that the text value comprises a combination of bi-grams that are not likely to
12 represent a genuine text value.

1 13. (Currently Amended) A method as recited in Claim 1, wherein determining the first
2 fraud risk score value comprises the steps of ~~the apparatus~~-determining a first fraud risk
3 score value associated with the electronic commerce transaction based on applying a
4 plurality of tests to the transaction data, by the steps of:
5 ~~the apparatus~~-receiving the name value;
6 for each bi-gram in the text value, ~~the apparatus~~-retrieving from a table of bi-gram
7 probability values a probability value that represents a probability that the bi-gram
8 is found in a genuine name value, wherein the table of bi-gram probability values
9 is created based on an actual frequency of occurrences of bi-grams in a large
10 sample of genuine names;

11 ~~the apparatus~~ generating a penalty value when the retrieved probability values indicate
12 that the text value comprises a combination of bi-grams that are not likely to
13 represent a genuine name value.

1 14. (Currently Amended) A method as recited in Claim 1, wherein determining the first
2 fraud risk score value comprises the steps of ~~the apparatus~~ determining a first fraud risk
3 score value associated with the electronic commerce transaction based on applying a
4 plurality of tests to the transaction data, wherein one of the plurality of tests automatically
5 determines whether a city value in the transaction data is within an area code value of the
6 transaction data, by the steps of:
7 ~~the apparatus~~ receiving the city value and the area code value as part of the transaction
8 data;
9 ~~the apparatus~~ determining a latitude value and a longitude value that represent a position
10 of a city identified in the city value;
11 ~~the apparatus~~ determining a range of latitude values and a range of longitude values
12 associated with an area code identified in the area code value;
13 based on the latitude value, the longitude value, the range of latitude values, and the range
14 of longitude values, ~~the apparatus~~ determining whether the city identified in the
15 city value is within the area code identified in the area code value;
16 ~~the apparatus~~ applying a penalty to the electronic commerce transaction when the city
17 identified in the city value is not within the area code identified in the area code
18 value.

1 15. (Currently Amended) A method as recited in Claim 1, wherein determining the first fraud
2 risk score value comprises the steps of determining a first fraud risk score value
3 associated with the electronic commerce transaction based on applying a plurality of tests
4 to the transaction data, wherein one of the plurality of tests automatically determines
5 whether a city value in the transaction data is within an email domain of the transaction
6 data, by the steps of:
7 ~~the apparatus~~ receiving the city value and an email address value as part of transaction
8 data;

9 ~~the apparatus~~ determining a latitude value and a longitude value that represent a position
10 of a city identified in the city value;
11 ~~the apparatus~~ determining a range of latitude values and a range of longitude values
12 associated with an email domain portion of the email address value;
13 based on the latitude value, longitude value, the range of latitude values, and the range of
14 longitude values, ~~the apparatus~~ determining whether the city identified in the city
15 value is within the email domain indicated in the email address value;
16 ~~the apparatus~~ applying a penalty to the electronic commerce transaction when the city
17 identified in the city value is not within the area code identified in the area code
18 value.

1 16. (Currently Amended) A method as recited in Claim 13, further comprising the steps of
2 ~~the apparatus~~ creating and storing an email domain location table comprising a plurality
3 of records that associate email domain values with city values associated with shipping
4 addresses of past non-fraudulent transactions.

1 17. (Currently Amended) The method as recited in Claim 14, wherein determining whether
2 the city identified in the city value is within the email domain comprises the steps of ~~the~~
3 ~~apparatus~~ determining whether the city value is for a city that is outside the email domain
4 as indicated by the records in the email domain location table.

1 18. (Currently Amended) A method as recited in Claim 1, wherein determining the first
2 fraud risk score value comprises the steps of ~~the apparatus~~ determining a first fraud risk
3 score value associated with the electronic commerce transaction based on applying a
4 plurality of tests to the transaction data, wherein one of the plurality of tests automatically
5 determines whether a country value in the transaction data is proximate to a bank
6 referenced in a bank identification number of a credit card number in the transaction data,
7 by the steps of:
8 ~~the apparatus~~ receiving the country value and a bank identification number of a credit
9 card number as part of the transaction data;

10 ~~the apparatus~~ determining a relative distance between a country identified in the country
11 value and a bank associated with the bank identification number;
12 based on the relative distance between the country and the bank, ~~the apparatus~~
13 determining whether the country is greater than a specified relative distance from
14 the bank;
15 ~~the apparatus~~ applying a penalty to the electronic commerce transaction when the country
16 is greater than the specified relative distance from the bank.

1 19. (Currently Amended) A method as recited in Claim 18, further comprising the steps of
2 ~~the apparatus~~ creating and storing a bank location table comprising a plurality of records,
3 wherein each record associates a bank identification number with a country value
4 representing a country in which a headquarters of the bank is located.

1 20. (Currently Amended) A method as recited in Claim 19, further comprising the steps of
2 ~~the apparatus~~ creating and storing a bank location table comprising a plurality of records
3 that associate bank identification numbers with country values associated with shipping
4 addresses of past non-fraudulent transactions.

1 21. (Currently Amended) The method as recited in Claim 20, wherein determining whether
2 the country identified in the country value is greater than the specified relative distance
3 from the bank comprises the steps of ~~the apparatus~~ determining whether the country value
4 is for a country that is greater than the specified relative distance from the bank as
5 indicated by the records in the bank domain location table.

1 22. (Currently Amended) A method of determining evaluating fraud risk of an electronic
2 commerce transaction, the method comprising the computer-implemented steps of:
3 ~~an apparatus~~ receiving transaction data that defines the electronic commerce transaction;
4 ~~the apparatus~~ determining a first fraud risk score value associated with the electronic
5 commerce transaction based on applying a plurality of tests to the transaction data,
6 wherein one of the plurality of tests includes at least:
7 ~~the apparatus~~ receiving the name value;

for each bi-gram in the text value, ~~the apparatus~~ retrieving from a table of bi-gram probability values a probability value that represents a probability that the bi-gram is found in a genuine name value, wherein the table of bi-gram probability values is created based on an actual frequency of occurrences of bi-grams in a large sample of genuine names;
~~the apparatus~~ generating a penalty value when the retrieved probability values indicate that the text value comprises a combination of bi-grams that are not likely to represent a genuine name value.

23. (Canceled)

24. (Previously Presented) A computer-readable medium carrying one or more sequences of instructions for evaluating fraud risk of an electronic commerce transaction, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:
receiving transaction information that defines the electronic commerce transaction;
determining a first fraud risk score value associated with the electronic commerce transaction based on applying a plurality of tests to the transaction data, wherein each of the plurality of tests determines whether the transaction data appears to represent a genuine transaction based on specified criteria;
determining a second fraud risk score value associated with the electronic transaction based on a comparison of the transaction information to historical transaction information;
combining the first fraud risk score value and the second fraud risk score value using a statistical model to result in creating a model score value;
blending the model score value with one or more merchant-specific threshold values to result in creating and storing a final fraud risk score value for the electronic commerce transaction.

1 25. (Previously Presented) An apparatus for evaluating fraud risk of an electronic commerce
2 transaction, the apparatus comprising:
3 means for receiving transaction data that defines the electronic commerce transaction;
4 means for determining a first fraud risk score value associated with the electronic
5 commerce transaction based on applying a plurality of tests to the transaction data,
6 wherein each of the plurality of tests determines whether the transaction data
7 appears to represent a genuine transaction based on specified criteria;
8 means for determining a second fraud risk score value associated with the electronic
9 commerce transaction based on a comparison of the transaction data to historical
10 transaction data;
11 means for combining the first fraud risk score value and the second fraud risk score value
12 using a statistical model to result in creating a model score value;
13 means for blending the model score value with one or more merchant-specific threshold
14 values to result in creating and storing a final fraud risk score value for the
15 electronic commerce transaction.

1 26. (Previously Presented) An apparatus for evaluating fraud risk of an electronic
2 commerce transaction, comprising:
3 a processor;
4 a computer readable medium having one or more sequences of instructions stored thereon
5 which, when executed by the processor, cause the processor to carry out the steps
6 of:
7 receiving transaction data that defines the electronic commerce transaction;
8 determining a first fraud risk score value associated with the electronic commerce
9 transaction based on applying a plurality of tests to the transaction data,
10 wherein each of the plurality of tests determines whether the transaction
11 data appears to represent a genuine transaction based on specified criteria;
12 determining a second fraud risk score value associated with the electronic
13 commerce transaction based on a comparison of the transaction data to
14 historical transaction data;

15 combining the first fraud risk score value and the second fraud risk score value
16 using a statistical model to result in creating a model score value;
17 blending the model score value with one or more merchant-specific threshold
18 values to result in creating and storing a final fraud risk score value for the
19 electronic commerce transaction.

1 27. (Currently Amended) A method of evaluating fraud risk of an electronic commerce
2 transaction, the method comprising the computer-implemented steps of:
3 ~~an apparatus~~ receiving transaction data that defines the electronic commerce transaction;
4 ~~the apparatus~~ determining a first fraud risk score value associated with the electronic
5 commerce transaction based on applying a plurality of tests to the transaction data;
6 ~~the apparatus~~ determining a second fraud risk score value associated with the electronic
7 commerce transaction based on a comparison of the transaction data to historical
8 transaction data;
9 ~~the apparatus~~ combining the first fraud risk score value and the second fraud risk score
10 value using a statistical model to result in creating a model score value;
11 ~~the apparatus~~ blending the model score value with one or more merchant-specific
12 threshold values to result in creating and storing a final fraud risk score value for
13 the electronic commerce transaction.

1 28. (Currently Amended) A method as recited in claim 1, wherein:
2 ~~the apparatus comprises a first apparatus and a second apparatus linked by a network;~~
3 ~~the apparatus~~ receiving the transaction data is performed by ~~the~~ a first apparatus that is
4 linked to a second apparatus by a network; and
5 ~~the apparatus~~ blending the model score value is performed by the second apparatus.

1 29. (Currently Amended) A method of evaluating fraud risk of an electronic commerce
2 transaction, the method comprising the computer-implemented steps of:
3 ~~an apparatus~~ receiving transaction data that defines the electronic commerce transaction;

4 ~~the apparatus~~ determining a first fraud risk score value associated with the electronic
5 commerce transaction based on applying a plurality of tests to the transaction data,
6 wherein each of the plurality of tests determines whether the transaction meets
7 specified criteria;
8 ~~the apparatus~~ determining a second fraud risk score value associated with the electronic
9 commerce transaction based on a comparison of the transaction data to historical
10 transaction data;
11 ~~the apparatus~~ combining the first fraud risk score value and the second fraud risk score
12 value using a statistical model to result in creating a model score value;
13 ~~the apparatus~~ blending the model score value with one or more merchant-specific
14 threshold values to result in creating and storing a final fraud risk score value for
15 the electronic commerce transaction.

- 1 30. (Previously Presented) A computer-readable medium carrying one or more sequences of
2 instructions for evaluating fraud risk of an electronic commerce transaction, when
3 executed by one or more processors, the computer readable medium comprising:
4 memory carrying one or more instructions that cause the one or more processors to carry
5 out the step of receiving transaction information that defines the electronic
6 commerce transaction;
7 memory carrying one or more instructions that cause the one or more processors to carry
8 out the step of determining a first fraud risk score value associated with the
9 electronic commerce transaction based on applying a plurality of tests to the
10 transaction information, wherein each of the plurality of tests determines whether
11 the transaction information appears to represent a genuine transaction based on
12 specified criteria;
13 memory carrying instructions one or more instructions that cause the one or more
14 processors to carry out the step of determining a second fraud risk score value
15 associated with the electronic transaction based on a comparison of the transaction
16 information to historical transaction information;

17 memory carrying instructions one or more instructions that cause the one or more
18 processors to carry out the step of combining the first fraud risk score value and
19 the second fraud risk score value using a statistical model to result in creating a
20 model score value; and
21 memory carrying instructions one or more instructions that cause the one or more
22 processors to carry out the step of blending the model score value with one or
23 more merchant-specific threshold values to result in creating and storing a final
24 fraud risk score value for the electronic commerce transaction.